



DEFENSE LOGISTICS AGENCY
DEFENSE ENERGY SUPPORT CENTER
8725 JOHN J. KINGMAN ROAD, SUITE 4950
FORT BELVOIR, VIRGINIA 22060-6222

DESC-I-23

December 17, 2009

BASE LEVEL SUPPORT APPLICATION (BLSA) ADMINISTRATOR PROCEDURES

References: See [Appendix 1](#)

1. GENERAL

a. **Applicability.** This procedural guidance is applicable to all Defense Fuel Support Points (DFSPs) that store Defense Working Capital Fund (DWCF) petroleum products including Government-Owned Government-Operated (GOGO), Government-Owned Contractor-Operated (GOCO), and Contractor-Owned Contractor-Operated (COCO) DFSPs managed by or contracted by Defense Energy Support Center (DESC) and the Military Services. This document was coordinated with the Military Service Control Points (SCPs) and approved by DESC as interim guidance pending inclusion to DoDM 4140.25, DoD Management of Bulk Petroleum Products, Natural Gas, and Coal.

b. **Supersession Date:** This administrative change supersedes DESC-I-23 dated November 13, 2009.

2. PROCESS. The purpose of this guidance is to define the BLSA Administrator's responsibilities and reduce the risk of fraud or error. With the absence of application level access controls, implement the guidance herein to the fullest extent possible.

3. RESPONSIBILITIES.

a. Responsible Officers (ROs), Terminal Managers (TMs), and Property Administrators (PAs) will:

(1) Identify and appoint DFSP personnel to serve as BLSA Administrators using the Delegation of Authority Letter format in [Appendix 2](#). This role should be restricted to the minimum number of users needed to support local mission requirements as determined by the RO, TM, or PA.

(2) Update the Delegation of Authority Letter within five business days upon addition to or removal of an individual from BLSA Administrator duties or every 12 months, whichever occurs first.

(3) Upon request, provide a copy of the Delegation of Authority Letter to the Defense Energy Support Center (DESC), DFSP Management (DESC-N) by email to DESC-TB@DLA.MIL or fax to commercial 703-767-8795 or DSN 312-427-8795.

(4) DFSPs shall request a waiver in accordance with [DESC-P-18, Request for Waiver and/or Exception to DoDM 4140.25-M](#) if they are unable to comply with any part of this instruction.

b. BLSA Administrator shall:

(1) Restrict system access to only DFSP personnel required to perform assigned duties.

(2) Complete a [DD Form 2875, System Authorization Access Request \(SAAR\)](#) for each user who requires access to the BLSA. Base access to FMD is on a verified need for access and grant in accordance with applicable laws and [DoD 5200.2-R, DoD Personnel Security Program](#). [Appendix 5](#) provides detailed instructions on how to complete this form.

(3) Locally maintain completed DD Forms 2875 on file for two years after account termination.

(4) Ensure all BLSA system users have read, understood, and signed the BLSA Information Assurance (IA): General Rules of Behavior package at [Appendix 4](#) prior to granting access to BLSA. Attach the completed General Rules of Behavior package to user's DD Form 2875 and maintain locally on file for two years after account termination. Be aware the BLSA does not authorize generic or group accounts.

(5) Delete or disable accounts immediately when personnel are no longer performing duties that require access to BLSA to include change in duty position, permanent change in station (PCS), and separation or retirement.

(6) Disable account in the event an employee has an extended absence such as TDY or leave and it will be more than 30 days before member will access the BLSA.

(7) Revalidate user privileges within BLSA annually at a minimum and determine whether access permissions are still required based on assigned duties and need-to-know requirements. This revalidation shall be formally documented and readily available to DFSP and DESC management. The evidence required is a current BLSA System Access Control Roster in the format prescribed in [Appendix 3](#). Retain evidence of annual revalidation until completing subsequent recertification.

(8) Serve as focal point between the [BSM-Energy Help Desk](#) and the host installation communications officials.

(9) Understand and follow the locally developed system disaster recovery and contingency plans for the host base network.

(10) Perform successful data backups and follow form disposition guidance in accordance with [DESC-P-3, Document/Data Control and Retention](#).

(11) Immediately report BLSA system failures to the [BSM-E Help Desk](#) and execute required corrective action and/or data restoration procedures as directed by the helpdesk personnel.

(12) Verify DoD approved virus protection software is loaded on BLSA computers and maintain current signature files.

(13) Report and follow-up on all system security incidents in a timely manner.

(14) Follow the host installation Incident Response Plan (IRP) and network enclave reporting procedures when a security incident occurs that affects and/or involves the BLSA or DESC owned workstation. In addition to IRP notification procedures, the BLSA Administrator shall notify the [BSM-Energy Help Desk](#) who will in turn notify the DLA Computer Emergency Response Team (CERT) and the BLSA Information Assurance Officer (IAO) regarding the incident.

(15) Adhere to role based access controls by granting and revoking personnel system access as necessary to support mission requirements. Only grant access to specific system roles required for DFSP personnel to accomplish assigned duties, also known as least privilege access. [Table 1](#) depicts groups, roles, and user permissions assigned within each FMD application.

(16) Contact the BSM-E helpdesk or reference the DESC COACH Web site at <https://ports2.desc.dla.mil/manuals/REF1111D.htm#> for more information regarding role based access controls.

(17) Maintain and use a separate user account with the least amount of access privileges when performing routine daily functions such as dispatch or accounting and non-administrative user roles within the BLSA.

4. **BACKGROUND.** The Base Level Support Application (BLSA) is composed of an integrated suite of Commercial Off-The-Shelf (COTS) software modules with the commercial name FuelsManager® Defense (FMD). These procedures exclude administration for Automated Fuel Service Station, Automated Data Collection, Automated Tank Gauging, Automated Fuel Handling Equipment, and FMD Express. The Base Level Support Application is the registered government name for this technology and is a subset of the Department of Defense (DoD) Business Systems Modernization – Energy (BSM-E) program. COTS small business-grade computer hardware hosts the BLSA that contains several modules to process a variety of functional tasks to support Defense Fuel Support Point (DFSP) management. The legacy BLSA application Fuels Control Center (FCC) is still in use but is in the phasing out process.

For Approval

//Signed Copy on File//

KIM J HUNTLEY
Director

OPR: DESC-N
OCR: DLA J-6F, DESC-G, O, R, Regions
SCP: AFPET, APC, NOLSC

Table 1: [FuelsManager® Defense Role Based Access Controls](#)
Appendix 1: [References](#)
Appendix 2: [BLSA Administrator Appointment Roster](#)
Appendix 3: [BLSA System Access Control Roster](#)
Appendix 4: [BLSA Information Assurance \(IA\): General Rules of Behavior](#)
Appendix 5: [BLSA Specific DD Form 2875 Instructions and Example](#)
Figure 1: [DD Form 2875 Example](#)

Table 1. FuelsManager® Defense Role Based Access Controls

Group	Read	Write	Configure	Operations
Administrator				
	X	X		Accounting
	X	X		Dispatch
	X	X		Equipment
	X	X	X	Maintenance
	X	X	X	Quality Control
	X	X		Scheduler
	X	X	X	Training
	X	X		Personnel
	X	X		Tank Inventory
	X	X		Reports
	X	X		Evacuate
Accounting				
	X	X		Accounting
	X			Equipment
	X			Tank Inventory
	X			Reports
	X			Scheduler
Contracting Officer Representative (COR)				
	X			Accounting
	X			Dispatch
	X			Equipment
	X			Maintenance
	X			Quality Control
	X			Scheduler
	X			Training
	X			Personnel
	X			Tank Inventory
	X			Reports
Dispatch				
	X	X		Dispatch
	X	X		Equipment
	X	X		Maintenance
	X	X		Quality Control
	X	X		Personnel
	X			Tank Inventory
	X			Reports
	X	X		Scheduler
	X	X		Evacuate
Equipment Status				
	X	X		Equipment
	X	X		Maintenance
	X	X		Quality Control
	X			Tank Inventory
	X			Scheduler
	X			Reports

Group	Read	Write	Configure	Operations
Inflights				
	X	X		Inflights
	X			Accounting
Maintenance				
	X	X		Maintenance
	X	X		Quality Control
	X			Tank Inventory
	X			Scheduler
	X			Reports
Personnel				
	X	X		Personnel
	X			Scheduler
	X			Tank Inventory
	X			Reports
Quality Assurance				
	X	X		Maintenance
	X	X		Quality Control
	X	X		Scheduler
	X			Tank Inventory
	X			Reports
Training				
	X	X		Training
	X	X		Scheduler
	X			Tank Inventory
	X			Reports
Trans Upload				
	X	X		Accounting
	X			Tank Inventory
	X			Scheduler
	X			Reports

Appendix 1

REFERENCES

- (a) [Air Force Instruction \(AFI\) 33-200, Information Assurance \(IA\) Management.](#)
- (b) [Army Regulation \(AR\) 25-2, Information Assurance.](#)
- (c) [Chairman of the Joint Chiefs of Staff Manual \(CJCSM\) 6510.01, Defense-In-Depth: Information Assurance \(IA\) and Computer Network Defense \(CND\).](#)
- (d) [Department of Defense Instruction \(DoDI\) 8500.2, Information Assurance \(IA\) Implementation, sections 5.11.2. and E3.4.7.](#)
- (e) [DoD 5200.2-R, DoD Personnel Security Program](#)
- (f) DLA One Book, Information Assurance (IA) Operational Controls.
- (g) [Office of the Chief of Naval Operations \(OPNAV\) Instruction 5239.1C, Navy Information Assurance \(IA\) Program.](#)
- (h) [Secretary of the Navy \(SECNAV\) M-5239.1, Information Assurance Manual.](#)
- (i) [DESC-P-3, Document/Data Control and Retention](#)
- (j) [DESC-P-18, Request for Waiver and/or Exception to DoDM 4140.25-M](#)

Appendix 2

BLSA ADMINISTRATOR APPOINTMENT ROSTER

MEMORANDUM FOR: DESC-N/DLA J-6

dd-mm-yy

FROM: enter organization name

SUBJECT: Appointment of BLSA Administrators

1. The following personnel shall serve as appointed Functional System Administrators in accordance with DESC-I-23, Base Level Support Application (BLSA) Procedures, for enter organization name.

PRIMARY

<u>Rank/Name (Last, First MI)</u>	<u>Office Symbol</u>	<u>Duty Phone</u>	<u>Position</u>	<u>Type of Investigation</u>	<u>Date of Investigation</u>	<u>Date Appointed</u>
-----------------------------------	----------------------	-------------------	-----------------	------------------------------	------------------------------	-----------------------

ALTERNATE(S)

<u>Rank/Name (Last, First MI)</u>	<u>Office Symbol</u>	<u>Duty Phone</u>	<u>Position</u>	<u>Type of Investigation</u>	<u>Date of Investigation</u>	<u>Date Appointed</u>
-----------------------------------	----------------------	-------------------	-----------------	------------------------------	------------------------------	-----------------------

Security Manager Signature: _____ Date: _____

2. BLSA computer names for which BLSA Administrator(s) are responsible to maintain is as follows.

Network Name/ID	Serial Number	Location	DESC or Base Owned

3. I acknowledge that BLSA Administrators are responsible for controlling access to the BLSA in accordance with DESC-I-23 and will coordinate all system requirements and issues between the host installation communications officials and the BSM-Energy Help Desk.
4. This letter supersedes previous letters and expires one year from the above date.
5. Please direct any questions to enter POC, E-Mail address, and phone number.

Responsible Officer/Terminal Manager Signature

Appendix 3

BLSA SYSTEM ACCESS CONTROL ROSTER

MEMORANDUM FOR: DESC-N/DLA J-6

dd-mm-yy

FROM: enter organization name

SUBJECT: BLSA System Access Control Roster

1. Base Level Support Application (BLSA) access is granted to the following personnel:

Name	Grade	BLSA User ID	Date Granted	Security Clearance	User Rolls Granted
Doe, Jane	E-4	U1234	1/1/2008	Top Secret	Dispatch, Accounting

2. Personnel granted BLSA access have authorized Need-to-Know and are only granted an access level necessary to accomplish assigned duties in accordance with DESC-I-23.

3. This letter supersedes previous letters and expires one year from the above date.

4. Please direct any questions to enter POC, E-Mail address, and phone number.

BLSA Application Administrator Signature
NAME, RANK, Branch of Service

Appendix 4

BLSA INFORMATION ASSURANCE (IA): GENERAL RULES OF BEHAVIOR

**Defense Logistics Agency (DLA)
Information Assurance (IA): General Rules of Behavior**

Introduction

The Rules of Behavior delineate the responsibilities and expectations of all individuals with access to DLA Information Technology (IT) systems. All individuals will review and provide a signature hardcopy, digital or electronic verification to these rules prior to authorize access the Base Level Support Application (BLSA). The DoD annual Information Assurance training reinforces the Rules of Behavior.

What is the purpose of the Rules of Behavior?

Rules of Behavior hold users accountable for their actions and responsible for securing Government data and resources.

What are Rules of Behavior?

Rules of Behavior summarize laws and requirements from various DoD and DLA policies in regards to authorized DLA IT system use. Rules of Behavior establish standards of conduct that are vital in the establishment of a sound IA program. The Rules of Behavior highlight the need for users to understand that taking personal responsibility for securing DLA IT resources is an essential part of their mission.

Who is covered by these rules?

The General Rules of Behavior apply to the DoD civilian, military, contractor, and foreign national workforce with access to DLA IT systems such as BLSA. This workforce should be fully aware of, and comply with DLA security policies, as well as related DoD policies.

What are the penalties for Noncompliance?

Noncompliance with these rules will result in various potential sanctions imposed on an individual commensurate to the level of the infraction. Depending on the employment category and the severity of the violation, sanctions may range from a verbal or written reprimand, removal of Information Technology (IT) system access for a specified period of time, reassignment to other duties, or termination. Misuse of Privacy Act, sensitive, and/or classified data may result in civil and criminal charges and/or fines.

General Rules of Behavior

Users will:

- Safeguard information processed, stored, and transmitted on DLA IT systems from unauthorized or inadvertent modification, disclosure, destruction, and use. DLA IT systems are for official use and authorized purposes in accordance with DoD 5500.7-R, Joint Ethics Regulation (JER), section 2-301 at http://www.defenselink.mil/dodgc/defense_ethics/ethics_regulation/index.html.
- Comply with safeguards, policies, and procedures to prevent unauthorized access to DLA IT systems.
- Comply with terms of software licenses and only use DLA-licensed and authorized software.
- Complete periodic IA awareness training when made available.
- Use Internet access and/or electronic mail (e-mail) services on BLSA workstations for non-official purposes only under the following circumstances:
 - Usage does not adversely affect employee performance or accomplishment of DLA or DoD mission.
 - Usage does not reflect adversely on DLA, DoD, or the Federal Government.
 - Usage will occur on breaks, lunch periods, and non-duty hours.
 - Usage shall not cause undue burden on the information system, incur significant additional costs to the Government, or create an appearance of impropriety.
- Encrypted and digitally sign sensitive information using a Common Access Card-based DoD Public Key certificate before transmitting data via the internet.
- Recognize the accountability assigned to each user and realize each user must have a unique ID to access the BLSA.
- Be aware BLSA computers record individual user activity to include Internet, Intranet sites visited, and files accessed.
- Immediately report known or suspected security incidents to the responsible Information Assurance Manager in accordance with the Local Computer Incident Response Guide.
- Lock workstation when unattended for an extended period.
- Log out prior to leaving workstation area at the end of shift.

- Scan files received from un-trusted sources prior to opening.
- Label sensitive media and remove sensitive information from hard disks sent out for maintenance.
- Not use BLSA computers to:
 - Knowingly view, receive, or transmit material with pornographic content.
 - Conduct illegal activities and soliciting for personal gain.
 - Download copyrighted software without express permission.
 - Download without ensuring protection against viruses.
 - Misrepresent personal opinion as official information.
 - Knowingly distribute chain letters, extremist or terrorist material advocating the violent overthrow of the government and/or material or jokes that demean or ridicule others based on race, creed, religion, color, sex, disability or national origin.
- Not engage in deliberate activities that overload network resources such as downloading large music or video files that would inhibit or prohibit network service to other users.
- Not share account passwords with anyone, including Personal Identification Numbers (PIN) for Common Access Cards (CAC) associated with Public Key Infrastructure (PKI).
- Not attach non-Government issued device such as personally owned Personal Digital Assistants (PDA), jump drives, wireless devices, MP3 players, digital cameras, and so forth to DLA IT systems without prior approval from the responsible Information Assurance Officer (IAO).
- Not install single-license software on shared hard drives (or servers).
- Not modify automated screen-lock functions performed by the IT system.
- NOT process classified information using BLSA.
- NOT use shared drives to relay Privacy Act data unless the data is password protected and the folder within the shared drive has access set up only for those authorized to access the data.

- Be cognizant of DLA and DoD IA policies.

DoD IT systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management purposes, to ensure protection against unauthorized access, and to verify security procedures, continuity planning, and operational security. Monitoring may include active attacks by authorized DLA personnel to test or verify adequate security controls are in place.

During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or transmitted via this IT system may be monitored.

I acknowledge receipt of the General Rules of Behavior, understand my responsibilities, and will comply with these provisions for DLA IT systems.

Print Name

Date

Signature/Electronic Verification of User

Organization/Field Activity Office Symbol

Appendix 5

BLSA SPECIFIC DD FORM 2875 INSTRUCTIONS AND EXAMPLE

General: It is mandatory to complete all blocks and they be completed according to the instructions on the back of the form along with the following DESC specific supplemental instructions. It is preferred the form be typed, however, if hand written ensure writing is clearly legible.

Top of Form

Line 1/First Box: Place an “X” in the appropriate box to indicate type of request, “Initial” “Modification” or “Deactivate.” If the requestor already has access to a DESC AIS, enter the User ID.

Line 1/Second Box: Enter the date of the request.

Line 2/First Box: Enter “Base Level Support Application”.

Line 2/Second Block: Enter the users DFSP Name.

Parts I and II:

Blocks 1-12: Complete blocks 1-12.

Block 6: Must be the e-mail address of the system user/requestor.

Block 10: Check one of the three boxes “Military”, “Contractor” or “Civilian”.

IA Training and Awareness Certification Requirement: Enter “X” in box and date IA training completion date. Training is required annually, thus completion date must be current (completion within last year of system access request date).

Blocks 11 and 12: Requestor must sign and date the form to certify personal information is correct, completion of the IA Training and Certification, and to acknowledge understanding of Rules of Behavior at [Appendix 5](#) regarding use of BLSA.

Block13: Use this block for a brief justification of the requirement.

Block 14: All field level users must check “Authorized.”

Block 15: Select “UNCLASSIFIED” box.

Block 16: Supervisor must check the box certifying user need-to-know.

Blocks 17-20: Completed by the user's supervisor. If the BLSA Application Administrator is also the user's immediate supervisor, another person in the user's chain-of-command shall sign as the supervisor.

Blocks 21-21b: Completed by the BLSA Application Administrator. Note: Different persons must complete and sign blocks 17-20 and 21-21b. If the BLSA Application Administrator is also the user's immediate supervisor, another person in the user's chain-of-command must sign as the supervisor.

Blocks 22-25: To be completed by the Fuels Responsible Officer.

Block 27: N/A.

Part III:

Blocks 28-32: Completed by the Military Service Security Monitor or Provost Marshal. Enter the specific type of investigation completed, date investigation was completed, clearance level if applicable, and IT Level the individual is eligible for in blocks 28a-28c. Enter the printed name and complete telephone number of the person verifying documentation of the background check in blocks 29-30. The person verifying the background investigation must sign block 31 and enter the date of the signature in block 32.

Part IV: Leave blank.

Figure 1 EXAMPLE ONLY

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)			
PRIVACY ACT STATEMENT			
AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.		PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.	
ROUTINE USES: None.		DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.	
TYPE OF REQUEST <input checked="" type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID			DATE (YYYYMMDD) 20091125
SYSTEM NAME (Platform or Applications) Base Level Support Application		LOCATION (Physical Location of System) (Your DFSP Name)	
PART I (To be completed by Requestor)			
1. NAME (Last, First, Middle Initial) Fuelman, John, J.		2. ORGANIZATION (Your Organization Name)	
3. OFFICE SYMBOL/DEPARTMENT		4. PHONE (DSN or Commercial) (xxx)xxx-xxxx	
5. OFFICIAL E-MAIL ADDRESS john.fuelman@basename.mil		6. JOB TITLE AND GRADE/RANK Logistics Analyst, GS-09	
7. OFFICIAL MAILING ADDRESS 1234 POL Road Your Place, Anywhere 22222		8. CITIZENSHIP <input checked="" type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER	9. DESIGNATION OF PERSON <input type="checkbox"/> MILITARY <input checked="" type="checkbox"/> CIVILIAN <input type="checkbox"/> CONTRACTOR
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) <input checked="" type="checkbox"/> I have completed Annual Information Awareness Training. DATE (YYYYMMDD) 20091030			
11. USER SIGNATURE			12. DATE (YYYYMMDD) 20091125
PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)			
13. JUSTIFICATION FOR ACCESS Access to BLSA is required to process and input transactions.			
14. TYPE OF ACCESS REQUIRED: <input checked="" type="checkbox"/> AUTHORIZED <input type="checkbox"/> PRIVILEGED			
15. USER REQUIRES ACCESS TO: <input checked="" type="checkbox"/> UNCLASSIFIED <input type="checkbox"/> CLASSIFIED (Specify category) <input type="checkbox"/> OTHER			
16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. <input checked="" type="checkbox"/>		16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)	
17. SUPERVISOR'S NAME (Print Name) MSgt David A. Gasman		18. SUPERVISOR'S SIGNATURE	19. DATE (YYYYMMDD) 20091125
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT		20a. SUPERVISOR'S E-MAIL ADDRESS David.Gasman@basename.mil	20b. PHONE NUMBER (703) 555-1212
21. SIGNATURE OF INFORMATION OWNER/OPR		21a. PHONE NUMBER (703) 555-1313	21b. DATE (YYYYMMDD) 20091125
22. SIGNATURE OF IA O OR APPOINTEE		23. ORGANIZATION/DEPARTMENT RO/PA/TM Office Symbol	24. PHONE NUMBER 555-1414
			25. DATE (YYYYMMDD) 20091125

DD FORM 2875, AUG 2009

PREVIOUS EDITION IS OBSOLETE.

Adobe Professional 8.0

EXAMPLE ONLY

EXAMPLE ONLY

26. NAME (Last, First, Middle Initial) Fuelman, John, J.			
27. OPTIONAL INFORMATION (Additional information)			
PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION			
28. TYPE OF INVESTIGATION NACI		28a. DATE OF INVESTIGATION (YYYYMMDD) 20090801	
28b. CLEARANCE LEVEL Secret		28c. IT LEVEL DESIGNATION <input type="checkbox"/> LEVEL I <input type="checkbox"/> LEVEL II <input checked="" type="checkbox"/> LEVEL III	
29. VERIFIED BY (Print name) Joe Security	30. SECURITY MANAGER TELEPHONE NUMBER (703) 555-1616	31. SECURITY MANAGER SIGNATURE	32. DATE (YYYYMMDD) 20091125
PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION			
TITLE:	SYSTEM	ACCOUNT CODE	
	DOMAIN		
	SERVER		
	APPLICATION		
	DIRECTORIES		
	FILES		
	DATASETS		
DATE PROCESSED (YYYYMMDD)	PROCESSED BY (Print name and sign)	DATE (YYYYMMDD)	
DATE REVALIDATED (YYYYMMDD)	REVALIDATED BY (Print name and sign)	DATE (YYYYMMDD)	
DD FORM 2875 (BACK), AUG 2009			Reset

EXAMPLE ONLY